PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)
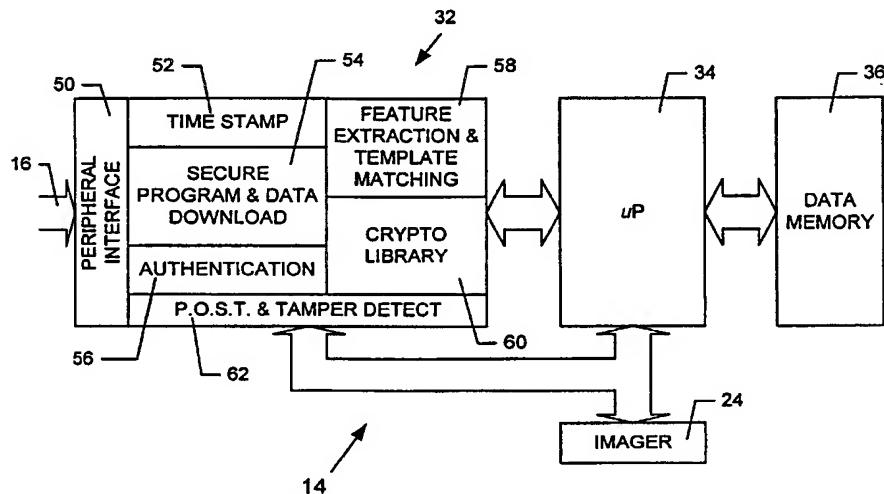
(54) Title: HIGH SECURITY BIOMETRIC AUTHENTICATION USING A PUBLIC KEY/PRIVATE KEY ENCRYPTION PAIRS

(57) Abstract

A trusted sensor (14) for authenticating biometric information used in an encryption system is provided. The trusted sensor (14) is disposed on at least one integrated circuit and comprises a microprocessor (34), and a data memory (36) coupled to the microprocessor (34). The data memory (36) is configured to hold a plurality of templates representing enrolled biometric information, a biometric public key and private key pair corresponding to each of the plurality of templates, and a manufacturer public key and private key pair. The trusted sensor (14) further comprises a functions section (32), also coupled to the microprocessor (34), which is configured to cause the microprocessor (34) to perform various functions. The functions section (32) includes a cryptographic library module (60), which stores one or more public key private key encryption functions and population functions for populating the biometric public key and private key pairs corresponding to each of the plurality of templates. The functions section (32) also includes a feature extraction and template matching module (58), which stores instructions for extracting features created with a biometric image capture device (24) coupled to the trusted sensor (14), and for populating the plurality of templates. Additional functions are also included in the functions section (32) for matching sensed biometric information communicated from the biometric image capture device (24) to the enrolled biometric information stored the data memory (36) and, based on the match, for selecting a particular biometric private key and private key pair that will be used in the encryption system. The functions section (32) also includes an authentication module (56), which stores instructions for certifying the trusted sensor (14) to a host computer by executing the one or more encryption functions stored in the cryptographic module (60) using the manufacturer private key and a host computer public key.

HIGH SECURITY BIOMETRIC AUTHENTICATION USING
A PUBLIC KEY/PRIVATE KEY ENCRYPTION PAIRS

BACKGROUND

1.   Field of the Invention

The present invention relates to public key encryption systems, e.g., those employing a public key/private key pair, and more specifically to a method and apparatus for increasing the security of authentication by employing a more tamper resistant biometric authentication system.

2.   Background Information

It is well known in the art of encrypting messages to utilize what are known as public key systems. In a public key cryptosystem, a plain text message may be encrypted by inputting the message and an enciphering key to an encryption algorithm. To decipher the message, the encrypted message is input to the inverse of the same algorithm along with a deciphering key. As with many encryption techniques, the encryption algorithm transforms of the plain text message in a manner that is so complicated that it is computationally infeasible to reverse the process even if the algorithm is known.

A peculiarity of public key systems is that it is also computationally infeasible to determine the deciphering key from the enciphering key. Consequently, in a public key cryptosystem, both the algorithm and the enciphering key may be made available to the public without jeopardizing the security of a message enciphered with the enciphering key. Hence the term "public key" for the enciphering key. The deciphering key, which is confidential, is known as a "private key". With a public key system, anyone who wishes to receive encrypted messages may make an encryption algorithm and a public key freely available.

A sender's authentication can also be achieved utilizing cryptographic systems. In a derived key system, where a sender and receiver utilizing public parts of their keys negotiate a transaction key, by that negotiation that can insure that only the two have the transaction key. However, if either has had its public key system private key compromised then the negotiation by encrypting a message with a key supposedly known

only to authorized persons will falsely tell the recipient that the message came from an authorized source.

In a public key cryptographic system, if the sender encrypts information using the sender's secret key, all recipients will be able to decipher the information using the

5   sender's public key, which is available to all. The recipients can be assured that the information originated with the sender, because the public key will only decrypt material encoded with the sender's private key. This also assumes, however, that the sender is the only one with access to the sender's private key. Since, presumably, only the sender has the private key, the sender cannot later disavow that he sent the information.

10   The use of encryption techniques provides a basis for creating electronic signatures to documents. At least two ways exist whereby encryption can be utilized to electronically "sign" a document. The first method is to encrypt the entire document using the signer's private key. The second is to encrypt only a message digest of the document. A message digest could be a hashing code or the like which produces a unique compressed coded

15   representation of the electronic content of the document. The integrity of the text of the document, as well as the identity of the sender, can be verified by sending an encrypted version of the code and having the receiver decrypt the hashing code and compare it to the hashing code developed on its end from the electronic content of the document as received. Those skilled in the art will appreciate the fact that a hashing code is particularly

20   well suited for these applications since a small change in the electronic content of the document results in a very large change in the hashing code. United States Patent No. 5,850,442, issued to Muftic on December 15, 1998, entitled SECURE WORLD WIDE ELECTRONIC COMMERCE OVER AN OPEN NETWORK ("the '442 patent"), discloses aspects of such a system.

25   Public key encryption software is widely available. For example, Pretty Good Privacy (TM) public key encryption software is available for non-commercial use over the Internet in a form published by Phillip Zimmerman. One version, is PGP version 2.6.2 of Oct. 11, 1994. It is available from the Massachusetts Institute of Technology at net-dis.mit.edu, a controlled FTP site that has restrictions and limitations to comply with

30   export control requirements. The software resides in the directory /pub/PGP. A fully licensed version of PGP for commercial use in the U.S.A. and Canada is available through

ViaCrypt in Phoenix, Arizona. The Federal Data Encryption Standard (DES) is a single key encryption system that is also publicly available in many forms.

However, these systems still assume that the sender was the rightful possessor of the private key. It is also subject to an interloper assuming the identity of the recipient and
5   falsely utilizing the recipient's published public key. The '442 patent proposes a solution to this latter problem by utilizing a third party "trusted agent" to certify the user of the public key. But the '422 patent also recognizes that even this is a compromising situation, since the typical access verification systems to obtain the trusted party certification are subject to compromise.

10   The '422 patent suggests utilizing a network including a plurality of user terminals connected to the network -- at least some of which are equipped with the ability to read and/or write smart tokens containing cryptographic keys. A plurality of servers and one or more security servers are also connected to the network. The security server certifies the public keys of users registered to engage in commercial transactions or the public keys of
15   other security servers. The network is arranged so that encryption keys from a smart token may be authenticated by one or more security servers and used to ensure the origin and authenticity of electronic transactions conducted using the user terminals and servers.

Public key encryption systems can be subject to a vulnerability involving the use of bogus time stamps. A user may alter the date and time setting of the user's systems clock
20   and generate either public key certificates or signatures that appear to have been created at a different time. The user can make it appear that a document was signed earlier or later than it was actually signed or sent. This may have some type of benefit, for example, by creating circumstances that might allow the user to repudiate a signature.

In some situations, where the generation of an accurate time stamp is not practical,
25   the art has substituted a monotonically increasing large number that can be used to place documents generated in a given order in that order when received.

In situations where it is critical that a signature has the correct date and time, or is otherwise to be placed in particular order, an electronic equivalent of a notary has been utilized in the art. An electronic notary, a third party trusted agent, would apply the
30   notary's electronic signature to other people's electronic signatures, thus witnessing the date and time of the signed document. A notary could actually maintain a log of detached signature certificates and make it available for public access. The notary's signature

would have a trusted time stamp, which might carry more credibility than a time stamp on the original signature alone.

Another certification proposal, Network Working Group Request For Comments No. 1422, dated February 1993, addresses privacy enhancement for Internet electronic

5   mail and particularly address certificate-based key management. These proposals incorporate concepts utilized in the X.400 Message Handling System model of CCITT Recommendation X.400, the directory system Recommendation X.500 and the CCITT 1988 Recommendation X.509 directed to an authentication framework.

Smart cards have been developed that include a processor and/or memory built into

10   a transport medium the size of a typical credit card. The processors in these cards can be programmed like any other computer to perform desired functions. Smart card readers are known that permit one to read the contents of a smart card, and to interact with the smart card to change its contents or to utilize digitally stored information on the card for authentication purposes.

15   The use of biometric sensors to create data that is later used to verify that another sensed sample of the biometric data identifies the individual providing the sensed data is known in the art. United States Patent No. 4,876,726, issued to Capello on October 24, 1989, entitled METHOD AND APPARATUS FOR CONTEXTUAL DATA ENHANCEMENT ("the '726 patent"), for example, discloses a fingerprint identification

20   system in which a fingerprint is digitized into an image consisting of pixels. That image data is compared to stored data representing many such fingerprints using a comparison algorithm to see if a match can be obtained.

U.S. Patent No. 5,832,091, issued to Tomko on November 3, 1998, entitled "FINGERPRINT CONTROLLED PUBLIC KEY CRYPTOGRAPHIC SYSTEM, ("the

25   '091 patent") discloses the use of an enrollment device which converts, e.g., a fingerprint, into a two-dimensional gray scale pixel representation. This data is transformed in a scrambled fashion unique to the enrollee and the descrambling information stored on a storage medium, e.g., a "smart card," the enrollee carries with him/her. Subsequently, the enrollee's biometric feature is sensed and the information on the smart card is used to

30   descramble the sensed data to find a match. If a match is found, the system at that point generates from the data representing the biometric identifier itself a public key/private key pair for the enrollee for purposes of encrypting/decrypting messages. However, since that

number is still used to generate a public key/private key pair, and only then is the public
key pair transmitted to system subscribers, if the individual with the "wrong" biometric
information gets the keys and is identified to the public-key encryption network as the
wrong person, then the benefits of a "public-key" cryptographic system would still be

5   available to the wrong possessor of the enrollee's smart card. That is to say, the biometric
identification system and its security measures seem to clearly identify the individual
subsequently as being or not being the "right" person having or not having the "right"
"unique number."

        The system of the '091 patent does not seem to deny access to the "public-key"

10   encryption system, but only to access to the system with the same keys as the "right"
holder of the smart card would have generated. Since the keys are only broadcast to the
other subscribers after this possibly false identification of the possessor of the smart card,
the smart card system of the '091 patent does not seem to provide authenticated uses of the
public key encryption system at all.

15   United States Patent No. 5,469,506, issued to Berson et al. on November 21, 1995,
entitled APPARATUS FOR VERIFYING AN IDENTIFICATION CARD AND
IDENTIFYING A PERSON BY MEANS OF A BIOMETRIC CHARACTERISTIC, ("the
'506 patent") discloses a system whereby the person wishing to have his/her identity
verified for access or other reasons carries a token, e.g., a card that contains magnetically

20   stored digitized data representative of a biometric previously scanned and recorded. A
similar scanner compares the data on the card to the scanned biometric data from the
bearer of the card to determine if there is a match. This form of system, however, even if
used for access to a private key of a public key/private key pair is still subject to the above
noted forms of security breach, in that a third party issuing the private key has access to

25   the public key/private key pair, and the token is subject to tampering.

        The same can be said for the system disclosed in United States Patent No.
5,280,527, issued to Gullman, et al. on January 18, 1994, entitled BIOMETRIC TOKEN
FOR AUTHORIZING ACCESS TO A HOST SYSTEM, ("the '527 patent"). The '527
patent discloses the use of fixed biometric data in combination with other random data to

30   obtain access to secure places, such as electronic financial transactions. The invention
supplants the user I.D., e.g., a "PIN," with biometric data previously recorded and stored
and uses a token for scrambling the transmission of the identification data back to a remote

site, e.g., the computer at the bank. Tokens scramble the PIN or other identifying data so unauthorized listeners cannot link the PIN to an account at the bank. In the '527 patent, biometric data is used as a "seed" for the random generation of the token. The system as disclosed uses a card storage to store the biometric data compared to the input at a remote

5   site from the host computer, e.g., at an ATM machine. The biometric comparison is done in the remote site, and simply acts as a more complex PIN.

United States Patent No. 5,245,329, issued to Gokcebay on September 14, 1993, entitled ACCESS CONTROL SYSTEM WITH MECHANICAL KEYS WHICH STORE DATA, ("the '329 patent") discloses the use of biometrics stored on a card carried by the

10   person to be identified against data scanned at the site to which access is sought, in combination with another item needed for access, such as a key or access card. This system also is subject to security breaches in that third parties also have access to whatever is kept in the site to which access is sought and the token is subject to tampering.

United States Patent No. 4,993,068, issued to Piosenka, et al. on February 12,

15   1991, entitled UNFORGEABLE PERSONAL IDENTIFICATION SYSTEM ("the '068 patent") discloses a similar system without the added access requirement, i.e., an additional key or access card.

Yet another similar system is disclosed in United States Patent No. 4,532,508, issued to Ruell on July 30, 1985, entitled PERSONAL AUTHENTIFICATION SYSTEM

20   ("the '508 patent") The '508 patent discloses a system wherein the contents of the token are further scrambled or encrypted in some fashion to prevent unauthorized use.

United States Patent No. 5,138,468, issued to Barbanell on August 11, 1992, entitled KEYLESS HOLOGRAPHIC LOCK ("the '468 patent"), also discloses the use of biometric data compared against stored data to provide identification and access.

25   United States Patent No. 5,268,963, issued to Monroe, et al. on December 7, 1993, entitled SYSTEM FOR ENCODING PERSONALIZED IDENTIFICATION FOR STORAGE ON MEMORY STORAGE DEVICES ("the '963 patent"), discloses a system wherein the biometric image data of an individual is encrypted by adding randomized unique serialized information according to a key derived from, e.g., the serial number of

30   the terminal that issued the personalized I.D. The system is designed to decrypt and reproduce the stored encrypted image as opposed to comparing it to stored biometric image data.

United States Patent No. 5,578,144 issued to Aucsmith, et al. on March 2, 1999, entitled DIGITAL CERTIFICATES CONTAINING MULTIMEDIA DATA EXTENSIONS ("the '144 patent"), discloses a system for creating and issuing a token ("digital certificate") for authentication of a person seeking remote access to stored data.

5   The "digital certificate" may include within it authenticating information, including biometric information. This information forms a "signature" that guarantees the authenticity of the certificate. The certificate also contains the public key encryption key of the authentic bearer.

United States Patent No. 5,872,848, issued to Romney, et al. on February 16, 1999,

10   entitled METHOD AND APPARATUS FOR WITNESSED AUTHENTICATION OF ELECTRONIC DOCUMENTS ("the '848 patent"), discloses a system employing a sort of digital "Notary Public" authenticating the "electronic" signature of the owner of an electronic document. The digital document is encrypted using the owner's private key corresponding to a public key. The "Notary" verifies that the "signature" was so done and

15   the identity of the owner (by usual documentary means or through biometrics), and attaches a digital "authenticator identification envelope" ("notary stamp") to the digital document. The "notary stamp" can also include biometric data identifying the owner.

United States Patent No. 5,872,849, issued to Sudia on February 16, 1999, entitled ENHANCED CRYPTOGRAPHIC SYSTEM AND METHOD WITH KEY ESCROW

20   FEATURE ("the '849 patent"), discloses a system for the secure generation, certification, storage and distribution of public-key encryption key pairs and for their escrow and public key certificate management.

The '849 patent also discloses the use of a "tamper-resistant" chip or a tamper-resistant trusted device containing the chip that performs the encryption, decryption and

25   digital signature according to a non-modifiable public/private signature key unique to the particular chip and with a "manufacturer's certificate." The chip "has the ability to use the device signature key [unique to the chip] to sign a request for certification of the user public signature key that it has generated for the user, thus proving that the user signature key pair was generated by, and the private key is being safeguarded by, a device of known

30   tamper-resistant properties." The system can generate public and private keys for a user and escrow them and certify the escrow. The system is immensely complicated in its escrowing features, including external escrowing and piece-wise escrowing, in order to

attempt to deal with governmental wiretap facilitation requirements. The system also is designed to escrow private keys for multiple users that can be accessed by the particular user upon presentation of some authentication, including password or PINs, but also including biometric input.

5   The '442 patent, mentioned above, discloses a system for ensuring that the user of a public key is indeed the registered user, and not an interloper. The system involves escrowing the public keys with a "trusted third party" and obtaining certification from the trusted third party that the user of the public key is the authentic one. The system uses a smart token for access management and control and the smart token can be uniquely

10   linked to its proper owner by biometric techniques, including biometric information stored on the card.

United States Patent No. 5,838,812 issued to Pare, Jr., et al. on November 17, 1998, entitled TOKENLESS BIOMETRIC TRANSACTION AUTHORIZATION SYSTEM ("the '812 patent") discloses a system that utilizes a remote computer to store

15   the biometric data to be compared with the user of the system seeking to authenticate his/her identity, as opposed to having the biometrics on the user's card ("token").

United States Patent No. 5,748,838, issued to Bisbee, et al. on May 5, 1998, entitled SYSTEM AND METHOD FOR ELECTRONIC TRANSMISSION, STORAGE AND RETRIEVAL OF AUTHENTICATED DOCUMENTS ("the '738 patent"),

20   discloses a system whereby a trusted third party acts essentially as a "notary" to authenticate the user of a cryptographic system by appending a digital signature of the third party to the document. To register with the third party the cryptographic user sends in its public key along with verification of the user's biometric information, which is then provided back to the user in the form of a token card to be used to access the system.

25   United States Patent No. 5,878,139, issued to Rosen on March 2, 1999, entitled METHOD FOR ELECTRONIC MERCHANDISE DISPUTE RESOLUTION ("the '139 patent"), discloses a system utilizing a third party trusted agents in supposedly tamper proof environment utilizing tamper-proof devices to act as electronic certifiers or intermediaries, e.g., for the purposes of facilitating a commercial transaction involving

30   real-time delivery of a product electronically and the real-time electronical payment.

All of the foregoing systems have drawbacks. Those systems that rely on third parties as trusted agents in either a certification or "notary public" type of role or act as

escrows for the secure information, such as a public key/private key pair, are only as tamper proof as the trusted agent chooses to make them. The trusted agent is subject to corruption and can falsely issue the certification or the escrowed keys. Those systems that rely on tokens are only as secure as the issuer of the token makes them. False tokens

5   identifying another individual, and incorporating the biometric data of the false individual are subject to being issued by the issuer or forgers as is the case with credit cards or check ·cards and, e.g., PIN, password or other identifiers (including biometrics) of the possessor of the token.

Furthermore, systems that encrypt the entire message or transaction information

10   are subject to the burgeoning efforts of the Federal government to preserve governmental access, thus requiring complex escrowing schemes to try to ensure only government access in addition to the authorized party encrypting the message or transaction. While such systems may be more "tamper proof" in that multiple third party agents would need to be corrupted, they are, nevertheless, complicated to use.

15   Moreover, the systems that distribute the biometric data of the enrollee to a third party escrow or notary can be corrupted to permit access to the biometric data of the enrollee by the government or other third parties without the authorization of the enrollee. Such access may be for unauthorized access to the enrollee's secure keys or information, or carrying out unauthorized transactions in the name of the enrollee. Therefore, the "non-

20   repudiation" feature reputed to public key/private key pair systems are not without the possibility of compromise through unauthorized access to the pair.

SUMMARY OF THE INVENTION

The present invention utilizes a trusted sensor contained within or peripheral to the

25   personal computer of enrollee. The enrollee is enrolled using an enrollment process that is unique to the enrollee's own personal trusted sensor to generate the public key/private key pair for the enrollee. The system employs integrated circuits contained within the computer, either consisting of the CPU of the computer or peripheral to the CPU (e.g., a co-processor), which enroll the enrollee by sampling a biometric of the enrollee and

30   storing the biometric for future comparison. The biometric is sampled by a suitable sampling device, for example, existing capacitive fingerprint detectors, which may utilize a CCD or CMOS digital imaging device. This may be incorporated into the computer,

9

(e.g., as part of the keyboard or CRT housing), or may be a stand alone peripheral connected to the computer through an input output port. The sampled biometric is converted into data indicative of the characteristics of the biometric so that it can be later used by the integrated circuit to verify a current user as being the enrollee. It is stored in

5   memory on the integrated circuit (or "chip"). The chip also generates a public key/private key pair that is verifiable as having been generated by the same chip that contains the biometric identifier of the enrollee. When the enrollee is ready to verify that a message or transaction is indeed sent from or being transacted by the enrollee, the enrollee has the appropriate biometric resampled. The biometric is converted to the identifying features

10   and compared to the data stored in the chip memory. The private key matching the enrollee is then produced by the chip. The enrollee never has to know or handle the secret "private key" or carry it around, thereby removing a possible source of compromise of the key. No third party is ever exposed to the private key or to the enrollee's biometric data.

        The public key/private key pair so generated can be utilized in a variety of ways,

15   but in the preferred embodiment it is utilized as an authorizing signature. The preferred embodiment utilizes a coded representation, such as a hashing code, of the particular message being transmitted (which can be a message otherwise sent in the clear or an electronic commercial transaction) and encrypts the hashing code with the private key. This encrypted hashing code is transmitted with the message, and if necessary with the

20   enrollee's public key. The recipient verifies the "signature" by decrypting the hashing code using the enrollee's public key and comparing it to the actual hashing code generated from the clear text message/transaction data. For added security other identifying information, such as a "date stamp" can be encrypted with the enrollee's private key, to be decrypted by the recipient.

25   In addition to certification of the source of a message or a transaction, the present invention is susceptible of other related uses. For example, the password or other access code for access (remote or otherwise) by an employee to the internal network of a company can be encrypted with the public key/private key pair generated by the system for the enrollee. This could also include special access codes or the like for especially

30   secure parts of the employer's network or databases or the like, for example research and development information, personnel files, etc.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a block diagram of the main elements of an embodiment of the present invention.

FIG. 2 shows a block diagram of the main elements of a secure or "trusted" sensor according to an embodiment of the present invention.

FIG. 3 shows a block diagram of the parties to the encryption scheme according to an embodiment of the present invention.

FIG. 4 is a flowchart illustrating the process for enrolling biometric information according to an embodiment of the present invention.

FIG. 5 is a flowchart illustrating the process of verifying a trusted sensor according to an embodiment of the present invention.

FIG. 6 is a flowchart illustrating the authentication or authorization process according to an embodiment of the present invention.

The use of similar reference numerals in different Figures indicates similar or identical items.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

FIG. 1 is a block diagram of an embodiment of the present invention. The public key access verification system 10 of the present invention includes a host computer 12, e.g., a desktop PC employing, e.g., a 32 bit Pentium II microprocessor or a 64 bit Pentium III RISC microprocessor, both made by Intel. The host computer 12 is connected to a trusted sensor 14 by a data transfer bus 16, e.g., a standard RS-232 or a Universal Serial Bus ("USB") serial data interface bus. Integrated into the host computer 12, e.g., as a part of its keyboard or its CRT display terminal, or interconnected to the host computer 12 as an external peripheral is a fingerprint image capture device ("ICD") or imager 24, which may be any of a number of digital imaging devices available on the market utilizing either Charge Coupled Device ("CCD") or CMOS digital imaging technologies known in the art. According to one embodiment, the imager 24 includes a fingerprint analyzer chip FPS110 available from Veridicom, Inc., or a similar capacitive fingerprint sensor as is disclosed in U.S. Patent Application Serial No. 08/855,230, filed May 13, 1997, which is incorporated herein by reference in its entirety.

The host computer 12 is connected through the public network, such as the Public Switched Telephone Network ("PSTN"), an intranet, the Internet or an equivalent public network 22 to a recipient computer 20.

Turning now to FIG. 2, the trusted sensor 14 is shown to include a functions
5   section 32, a microprocessor 34, and a data memory 36.

The microprocessor can be an off-the-shelf microprocessor, e.g., a Pentium II or III, an NEC VR4121, a Philips P38W858 secured controller or a Philips HSIS/IR9802 Smart XA Microcontroller. Alternatively, the microprocessor 34 can be a DSP, e.g., an ADSP 2141 provided by Analog Devices, or it can be a customized 16-, 32- or 64-bit
10 architecture microprocessor core or Digital Signal Processor ("DSP") available from ATMEL or Analog Devices. The microprocessor 34 can also include or be connected to an address and control chip which also contains assorted "glue" logic, as is known in the art, and identified as a 29LV160B or an AM29LV800BB120 EC available from AMD or an ST M29W800AB120 available from SGS Thompson.

15 The data memory 36 can be virtually any off-the-self ROM, EPROM or the like, along with RAM. According to one embodiment, the data memory 36 includes a 4Mx16 SDRAM, e.g., a PD4564163G5-A10L-9JF memory chip available from NEC.

In the embodiment shown in FIG. 2, the fingerprint image capture device 24 is communicatively coupled directly to the microprocessor 34 within the trusted sensor 14.
20 The data memory 36 is also coupled to the microprocessor 34 and can also be coupled to the functions module 32. According to one embodiment, the image capture device 24 is coupled to the microprocessor 34 and the functions section 32.

The functions section 32 is a graphical representation of a set of functionalities performed within the trusted sensor 14 that may be implemented in application software
25 run on the microprocessor 34, or in firmware, including some specialized hardware circuitry not ordinarily part of a microprocessor architecture and adapted to facilitate fingerprint analysis and/or matching, large random number generation, exponentiation, encryption and the like.

The functions section 32 includes a peripheral interface 50 to the host computer 12
30 over the bus 16, which may be a serial interface such as an RS-232, USB or a bus level bus like ISA or PCI, with the preferred embodiment comprising an ISA interface. The peripheral interface 50 is essentially a communications protocol interface to the outside

12

world, for example with an associated host computer that manages the formatting and synchronization of the input and output data transfers to and from the trusted sensor 14.

The function section 32 also includes a secure time stamp generator or monotonically increasing number generator 52.

5   In addition, the functions section 32 includes a secure data and program download module 54. The secure data and program download section 54 is one of a number of currently available security functionalities for ensuring that the internal workings of the trusted sensor 14 are not corrupted by unauthorized modifications various modules of the functions section 32 or through the introduction of false data, e.g., biometric image data.

10   The authentication module 56, also an element of functions section 32, includes software for communicating with the host computer 12 and certifying that the trusted sensor 14 is the genuine trusted sensor. The host computer 12 contacts the microprocessor 34 within the trusted sensor 14 utilizing the software and communication protocols within the authentication module 56 and transmits to the microprocessor 34 a large randomly

15   generated number encrypted by a public key associated only with the manufacturer of the trusted sensor 14 or with the trusted sensor 14 itself. The microprocessor 34 within the trusted sensor 14 decrypts the encrypted number using its unique private key, paired with the manufacturer public key or the public key unique to the trusted sensor 14. The private key for each trusted sensor 14 is unique to the sensor and only available within the sensor.

20   The private key of the trusted sensor 14 is established at the time of its manufacture by the manufacturer. The microprocessor 34 within the trusted sensor 14 then modifies the large random number in some easily identifiable fashion, e.g., by adding a fixed number such as 1 to the large random number, encrypts it using the known public key of the host computer 12 and retransmits this modified number to the host computer 12. Upon receipt, the host

25   computer 12 decrypts the modified large random number and verifies the expected modification, thereby assuring that the trusted sensor 14 is the right trusted sensor 14. A diagramatic representation of the authentication module 56 described above is resented below with reference to FIG. 5.

A fingerprint (or other biometric) feature extraction and template matching module

30   58 is also included in the functions section 32. The feature extraction module 58 is one of a number of fingerprint or other biometric identification algorithms in use on the market today for generating from a digital image of the features of the biometric a "template" of

identifying aspects and for analyzing whether a sensed template matches a stored template. An embodiment of such a matching module 58 (and a multidimensional fingerprint constellation) are described in U.S. Patent Application Serial No. 09/354,929, filed July 15, 1999, entitled METHOD AND SYSTEM OF FINGERPRINT TEMPLATE

5   MATCHING, as well as U.S. Patent Application Serial No. 09/501,355, filed February 9, 2000, entitled BIOMETRIC FALSE ACCEPT DETECTION, which are both incorporated herein by reference in their entirety.

The functions section 32 also has a cryptographic library 60. The crypto-library 60 utilizes, for example, software cryptographic functions of Cryptolib 1.1 by Jack Lacy of

10   AT&T Bell Labs. Other examples of cryptographic software packages and functionalities that can be employed are Arbitrary length Bignums; bigmath package, including, bigAdd, bigSubtract, bigMultiply, bidDivide, bigRightShift, bigLeftShit, bigAnd, bigOr, bigXor, bigCopy, Euclid's extended GCD, and modular reduction and exponentiation; crypto primitives, including, DES and 3DES + modes, Diffie-Hillman, DES (signing and

15   verification roughly equivalent), El Gamal, Rabin's scheme, Random number generation (pseudo and true), MD [2,4,5], prime generation, RSA, SHA, truerand (for UNIX, Windows NT and Windows 95), quantization (for defense against Kocher's timing attack) and quantized RSA, DSA and El Gamal private key operations; and support functions, including, asn1.c, ioutils.c and netIface.c. Examples of computation times of some of

20   these modules and/or functionalities are shown below.

Table I contains representative times using different software and different computers for the bigPow times (a^b mod c, with a, b and c the same length, i.e., 512 and 1024 bits).

Table 1

512 bits	1024 bits	Machine
.12s	.72s	Sparc II (Brickell BigPow)
.43s	3.0s	Sparc II w/asm (gcc)
.12s	.78s	Sparc 10 w/asm (gcc)
.03s	.17s	Sparc 10 w/asm (Brickell BigPow)
.084s	.45s	SGI 150 Mhz Indigo
.109s	.75s	100 Mhz Pentium (gcc under DOS)

Table II shows times for StrongPrime generation with ProbTestAttempts = 5 and 100 primes generated per test. The times shown are total test time divided by 100 to give an average time per prime generated using Gordon's strong prime algorithm.

Table II

256 bits	512 bits	1024 bits	Machine
2.8s	24.0s	5.11m	Sparc II
.45s	2.7s	77s	100Mhz Pentium

Table III shows encryption and decryption times for encrypting a typical hashing code of 160 bits in length with an RSA 64 bit public exponent.

Table III

Function	512 bits	768 bits	1024 bits	Machine
encrypt	30ms	50ms	80ms	Sparc II
decrypt	160ms	480ms	930ms	Sparc II
encrypt	15ms	33ms	56ms	100 MHz Pentium (NT)
decrypt	38ms	104ms	214ms	100 MHz Pentium (NT)

Table IV shows sign and verify times for DSA.

Table IV

Function	512 bits	768 bits	1024 bits	Machine
sign	99ms	166ms	216ms	Sparc II (Brickell speedup)
verify	156ms	316ms	416ms	Sparc II (Brickell speedup)
sign	21ms	38ms	49ms	100 Mhz Pentium (NT)
verify	27ms	43ms	71ms	100 Mhz Pentium (NT)

The functions section also includes a (Power On Self Test) P.O.S.T. and tamper detect module 62. The P.O.S.T. and tamper detect module 62 implements any of a number of well-known P.O.S.T. system tests on power on and also any of a number of well-known tamper detect programs. For example, the FIPs 140 tamper detection and resist protocols, can be implemented, which can detect unauthorized attempts to crack into the trusted sensor 14 and either record them for subsequently informing the enrollee of such attempts or actively resist them by, for example, erasing stored secure information such as templates and private keys so that unauthorized access is prevented.

The physical integrated circuit or circuits constituting the trusted sensor 14 are themselves packaged in any of a number of well-known tamper resistant packaging methodologies, which, e.g., cause physical destruction to an integrated circuit, or in the case of EPROM's and the like, destroy the secure information stored in the memory of the integrated circuit in the event that a attempt is made to electronically access the memory without a properly encrypted access code, or an attempt is made to physically extract the integrated circuit from the packaging.

Some other functionalities to the functions section 32 of the present invention, excepting a secure, tamper-resistant memory, can be found in the N*Click product, which is described at http://www.nabletech.com.

In operation, the trusted sensor 14 is used to enroll an enrollee and to generate a public key/private key pair unique to the enrollee and/or unique to the specific biometric used (right thumb, left thumb, right eye, etc.). The trusted sensor returns the encrypted template to the host computer 12 or to another apparatus, for example, for the generation of a token (or smart card) for the enrollee, an encrypted version of the enrollee's template for the particular biometric. The host computer 12 may store this encrypted biometric data also. The biometric template is encrypted using the private key specific to the entrusted

sensor 14 (the private key being fixed in the trusted sensor 14 at manufacture) and is then transmitted to the host computer 12 using the host's public key. The microprocessor 34 also generates a registration certification for the generated public key for the host computer 12 to transfer to a recognized public key registration entity.

5   The enrollment process described above is depicted in FIG. 4 and discussed below. However, before turning to FIG. 4, it is useful to present a figure depicting an overview of the system first shown in FIG. 1 and described throughout this specification. For this we turn to FIG. 3.

         FIG. 3 depicts a convenient view of the overall framework and inter-operating

10   elements of the biometric encryption system. Shown in FIG. 3 are not only the elements described with reference to FIG. 1, but the various public key/private key pairs described elsewhere in this specification. Because the connection of the elements was previously described with reference to FIG. 1, it is not further belabored here.

         The host computer 12 includes a public key 42 and a private key 44. Similarly, the

15   remote computer 20 includes a public key 46 and a private key 48. Moreover, the trusted sensor 14, which may or may not directly include the imager 24, includes multiple sets of public keys and private keys. First, the trusted sensor 14 includes the public key 38 and private key 40 of the manufacturer of the trusted sensor 14. The manufacturer public key 38 and private key 40 can be associated with the imager 24, or they can be the public

20   key/private key 30 pair for the feature extraction and template matching module 58. Second, the trusted sensor 14 includes a public key 28 and private key pair for each biometric template 26 (for example a fingerprint constellation) stored in the trusted sensor 14. Multiple sets of public key/private key pairs can be stored in the trusted sensor 14 -- one for each specific template/biometric used.

25   Now turning to FIG. 4, which depicts the enrollment process described above, at step 64 the imager 24 captures biometric information, for example, using a capacitive fingerprint sensor such as the Veridicom, Inc. part no. FPS110. Features are extracted from the image, for example by feature extraction and template matching module 58 and a template (for example a fingerprint constellation) is generated in step 66. Next, a public

30   key 28 private key 30 pair is generated for the captured biometric information. This pair is stored in the trusted sensor 14. In step 70, a registration certificate is generated that includes the public key 28. In step 72 the registration certificate (including the public key

28) is set to a registration authority, preferably connected to public network 22. When sending the public key 28 to the registration authority, the host computer 12 is used as an intermediary, as the trusted sensor 14 is not necessarily directly connected to the public network 22. Once the public key 28 and private key 30 are generated and the public key

5   28 is sent to the registration authority, the biometric information is enrolled.

Now turning to FIG. 5, it depicts the sensor verification process described above. For convenience, it is set forth again here. In step 73, the host computer 12 generates a random number. The random number is encrypted with the public key 38 and private key 44 at step 74. In step in step 76, the encrypted random number is sent from the host

10   computer 12 to the trusted sensor 14. In step 80, the trusted sensor 14 receives the encrypted random number and, in step 82, decrypts the random number using the private key 40 and public key 42. Next, in step 84, the random number is modified. In step 86, the modified random number is then encrypted with the private key 40 and the public key 42 and then sent to the host computer 12 at step 88. In step 90, the encrypted modified

15   random number is received from the trusted sensor 14 and decrypted, in step 92, with the private key 44 and public key 38. The modification to the random number is verified by the host computer 12 in step 94, and if it matches the original random number generated at step 73, then the sensor 14 is then verified to be the trusted sensor 14. Now the trusted sensor 14 is ready for operation in the system 10.

20   It is noted that in step 73, the host computer can be an intermediary between the remote computer 20 and the sensor 14. In such an embodiment, the remote computer 20 can generate the random number or a hashing code and it is this value, encrypted by the remote computer 20 with the public key 38 and, of course, the private key 48, that can be verified through the process described above.

25   Thereafter, the enrollee presents his/her appropriate biometric to the image capture device at the host computer 12 or the trusted sensor 14. A template is generated from the input biometric image data. Upon verification of a match with an enrolled template 26, the trusted sensor 14 selects the private key 30 unique to the enrolled template 26. This private key 30 can be used to encrypt an entire message provided by the host computer 12

30   to the trusted sensor 14 for transmission back to the host computer 12. The host computer can then transmit the encrypted message to the intended recipient. For this purpose the host computer also transmits to the trusted sensor 14 the public key 46 of the recipient.

More conveniently, the host computer 12 transmits to the trusted sensor 14 a coded representation of the message to be sent, e.g., a hashing code of the message, and the trusted sensor 14 uses the generated private key 30 to encrypt the hashing code and transmits the encrypted message to the host computer 12 for transmission along with the

5   message. The recipient of the message creates an identical hashing code of from the received message and decrypts the encrypted hashing code and compares the two. An identical match insures that the message was received from the registered owner of the public key. In a similar manner, the trusted sensor 14, may encrypt a date stamp or a large monotonically increasing number provided by the date stamp module 52 and transmit the

10   value to the host computer 12 for inclusion in the message.

In operation, therefore, the trusted sensor 14 is only able to be accessed by a host computer 12 with the manufacturer or trusted sensor 14 specific public key, and the trusted sensor 14 responds only to such a host computer 12. Upon the production of the appropriate biometric image either by the host computer 12 or directly by the trusted

15   sensor 14, the trusted sensor 14 processes the image from the ICD and creates the distinguishing template. If the distinguishing template matches a stored template within the trusted sensor 14 the stored public key/private key pair of the enrollee is accessed.

The secure interface between the enrollee's host computer 12 and the trusted sensor 14 using the manufacturer or sensor public key and the paired private key within

20   the trusted sensor 14 ensures certification of the message and authenticated access only by the real enrollee having the proper biometric matching the internally stored template. The recipient, knowing that it is communicating with a machine using the manufacturer's (or sensor specific) public key 38/private key 40 pair, is assured that the sending host computer 12 has authenticated the use by the proper enrollee.

25   The overall authentication process described above is depicted in FIG. 6. It is assumed for purposes of this explanation that some triggering event, for example an interrupt from the remote computer 20 (or "intended recipient") has caused the trusted sensor 14 to become active.

In step 100, the sensor 14 performs the power on self-test (POST) using module

30   62. In step 102, using the process described above, for instance in FIG. 5, the sensor 14 is verified by the host computer 12. In step 104, the imager 24 collects biometric information and the trusted sensor 14 will match the biometric information (a template) to

a stored template 26. In step 106, assuming a successful match at step 104, the trusted sensor 14 selects the private key 30 corresponding to the matched stored template 26.

In step 108, the host computer 12 sends a hashing code or some other coded representation of the message to be returned to the remote computer 20, together with the remote computer 20 public key 46 to the trusted sensor 14. (It is noted that step 108 can be the triggering event that initiated the overall process earlier described above and shown in FIG. 6.) The trusted sensor 14, having been verified in step 102, encrypts the message using the biometric (e.g., fingerprint) template 26 private key 30 and intended recipient public key 46 in step 110. In step 112, the trusted sensor 14 sends the encrypted message to the host computer 12, which then re-transmits the encrypted message to the remote computer 20 in step 114. In step 116, the remote computer 20 verifies the encrypted message by decrypting it using the template public key 28 and the remote computer private key 48. When the message is verified, the authorization from the enrolled user of the trusted sensor 14 is confirmed.

A system as described above is highly useful in an environment where non-repudiation of a contract, or affirmation of a transaction with a remote user is desired. For example, the system can be implemented in a wireless telephone, a personal digital assistant, or a laptop or desktop computer. In such an instance, the host computer 12 would be the particular electronic device the trusted sensor 14 is incorporated into. For instance, the system can be incorporated into any of the electronic devices described in U.S. Patent Application Serial No. 09/536,242, filed March 27, 2000, entitled BIOMETRIC SENSING AND DISPLAY DEVICE, which is incorporated herein by reference in its entirety.

CLAIMS

What is claimed is:

1.   A trusted sensor (14) for authentication of biometric information used in an encryption system, said trusted sensor (14) disposed on at least one integrated circuit and

5   comprising:

a microprocessor (34);

a data memory (36) coupled to said microprocessor (34) and configured to hold a plurality of templates representing enrolled biometric information, a biometric public key private key pair corresponding to each of said

10   plurality of templates, and a manufacturer public key and private key pair; and

a functions section (32) coupled to said microprocessor (34), said functions section comprising:

a cryptographic library module (60) storing one or more public key private

15   key encryption functions and further storing instructions for causing said microprocessor (34) to populate said biometric public key and private key pair corresponding to each of said plurality of templates;

a feature extraction and template matching module (58) storing instructions for causing said microprocessor (34) to extract features created with

20   a biometric image capture device (24) coupled to said trusted sensor (14) and to populate to at least one of said plurality of templates, and further storing instructions for causing said microprocessor (34) to match sensed biometric information, communicated from said biometric image capture device (24), to said enrolled biometric

25   information stored said data memory (36) and, based on said match, select a particular biometric private key; and

an authentication module (56) storing instructions for causing said microprocessor (34) to certify said trusted sensor (14) to a host computer by executing said one or more encryption functions stored

30   in said cryptographic module (60) using said manufacturer private key and a host computer public key.

2.   The trusted sensor of claim 1, said authentication module (56) further storing instructions for causing said microprocessor (34) to execute said one or more encryption functions stored in said cryptographic library module (60) using said particular biometric private key, a public key corresponding to a remote computer, said one or more encryption functions encrypting a message destined for said remote computer.

3.   The trusted sensor of claim 2:
            wherein said biometric image capture device (24) includes a plurality of capacitive
                  fingerprint sensing elements; and
            wherein said manufacturer public key and private key pair correspond to said
                  plurality of capacitive fingerprint sensing elements.

4.   The trusted sensor of claim 2:
            wherein said biometric image capture device (24) includes a plurality of capacitive
                  fingerprint sensing elements; and
            wherein said manufacturer public key and private key pair correspond to said
                  functions section (32).

5.   The trusted sensor of claims 3 or 4, said functions section further comprising:
            a power on self-test and tamper detect feature (62) storing instructions for causing
                  said microprocessor (34) to enable said trusted sensor (14) when said power
                  on self-test is successful and said tamper detected feature detects no
                  tampering;
            a secure time stamp module (52) storing instructions for causing said
                  microprocessor (34) to generate a time stamp used by said authentication
                  module (56); and
            a peripheral interface (50) configured to communicatively couple microprocessor
                  (50) to said host computer over a secure communications link (16).

6.   A method for authenticating the identity of an individual in a transaction using a trusted sensor (14), the method comprising:
            performing a power on self-test on said trusted sensor (14);

verifying said trusted sensor (14) to a host computer (12) coupled to said trusted

sensor (14), said step of verifying using a manufacturer private key (40)

and a host computer public key (42);

receiving biometric information from an image capture device (24);

5 matching said biometric information from said image capture device (24) to an

enrolled biometric template (26) stored in said trusted sensor (14);

selecting a public key (28) and private key (30) pair corresponding to said enrolled

biometric template (26), said public key (28) and private key (30) pair

stored in said trusted sensor (14);

10 receiving a message from said host computer (12), said message including a

remote computer public key (46);

encrypting at least a portion of said message using said selected private key (30)

and said remote computer public key (46); and

sending said encrypted message from said trusted sensor (14) to said host computer

15 (12).

7. The method of claim 6, said step of verifying comprising:

receiving an encrypted random number from said host computer (12), said

encrypted random number encrypted by said host computer (12) using a

20 host computer private key (44) and a manufacturer public key (38);

decrypting said encrypted random number into a random number using said host

computer public key (42) and said manufacturer private key (40);

modifying said random number;

encrypting said modified random number using said manufacturer private key (40)

25 and said host computer public key (42); and

sending said encrypted modified random number to said host computer (12).

8. The method of claim 7, further comprising steps performed by said host computer

(12), said steps comprising:

30 generating said random number;

encrypting said random number using said host computer private key (44) and said

manufacturer public key (38) to form said encrypted random number;

sending said encrypted random number to said trusted sensor (14);

receiving said encrypted modified random number from said trusted sensor (14);

decrypting said encrypted modified random number using said host computer

private key (44) and said manufacturer public key (38); and

5   verifying said modification performed by said trusted sensor (14) to said random

number.

9.   The method of claim 8, further comprising steps performed by said remote

computer (20), said steps comprising:

10   encrypting a primary message with a remote computer private key (48) and a

transaction public key, said transaction public key selected from a group

comprising said host computer public key (42) and said selected public key

(28);

receiving a confirmation message from said host computer (12), said confirmation

15   message comprising said portion of said message encrypted at said trusted

sensor (14) using said selected private key (30) and said remote computer

public key (46); and

decrypting said portion of said confirmation message using said selected

transaction key and said remote computer private key (48).

20

10.   One or more computer readable mediums having stored therein one or more

sequences of instructions for causing one or more microprocessors to perform the steps

described in any of above claims 6 through 9.

25   10.   A high security biometric authentication system (10) using public key private key

pairs comprising:

a remote computer (20) including a remote computer public key (46) and private

key (48) pair;

a host computer (12) coupled to said remote computer (20), said host computer

30   (12) including a host computer public key (42) and private key (44) pair;

a biometric image sensing means (24) including a plurality of capacitive sensing elements for measuring relative distances between ridges and valleys on a fingerprint; and

a trusted sensor (14) coupled to said biometric image sensing means (24) and said host computer (12), said trusted sensor (14) including a microprocessor (34), a functions section (32) accessible by said microprocessor (34), and a data memory (36) including a plurality of biometric templates (26), each of said plurality of biometric templates (26) having a biometric template public key (28) and private key (30) pair, and a manufacturer public key (38) and private key (40) pair, wherein biometric information sensed by said biometric image sensing means (24) is manipulated and stored in said plurality of biometric templates (26), and wherein each of said biometric template public key (28) and private key (30) pairs is dependent upon said manipulated biometric information stored in corresponding one of said plurality of biometric templates (26).

12.   The high security biometric authentication system (10) of claim 11, wherein said trusted sensor (14) is verified by host computer (12) by:

sending a first message from said host computer (12) to said trusted sensor (14), said first message encrypted with said host computer private key (44) and said manufacturer public key (38);

receiving said first message at said trusted sensor (14), decrypting said first message, manipulating a portion of said first message, returning a return first message to said host computer (12), said return first message including said manipulated portion of said first message and said return first message encrypted with said manufacturer private key (40) and said host computer public key (42); and

receiving said return first message from said trusted sensor (14) at said host computer (12), decrypting said return first message with said host computer private key (44) and said manufacturer public key (38) and verifying said manipulation to said portion of said first message.

13.   The high security biometric authentication system (10) of claim 12, wherein a
transaction is verified, after first verifying said trusted sensor (14), by:

        sensing current user biometric information using said biometric image sensing
               means (24);

5

        comparing said current user biometric information to said plurality of biometric
               templates (26);

        selecting a particular biometric image template that matches said current user
               biometric information, said act of selecting including identifying a
               particular biometric public key and private key pair corresponding to said

10

               particular biometric image template;

        encrypting a second message authorizing a transaction with said particular
               biometric private key and said remote computer public key (46);

        sending said second message to said host computer (12);

        receiving said second message from said trusted sensor (14) at said host computer

15

               (12);

        re-transmitting said second message from host computer (12) to said remote
               computer (20);

        receiving said re-transmitted second message from host computer (12) at said
               remote computer (20); and

20

        verifying said re-transmitted second message using said host computer private key
               (48) and said particular biometric public key.

14.   The high security biometric authentication system (10) of claim 13:

        wherein prior to said step of re-transmitting said second message, said host

25

               computer encrypts said second message using said host computer private
               key (44) and said remote computer public key (46); and

        wherein said step of verifying said re-transmitted second message includes
               verifying said second message using said host computer public key (42).

1/5

FIG. 1

FIG. 2

2/5

FIG. 3

3/5

ENROLL

64 — CAPTURE
BIOMETRIC
INFORMATION

66 — GENERATE
TEMPLATE

68 — GENERATE
TEMPLATE PU_K
PR_K PAIR FOR
BIOMETRIC

70 — GENERATE
REGISTRATION
CERTIFICATE

72 — SEND TEMPLATE
PU_K TO
REGISTRATION
AUTHORITY

ENROLLED

FIG. 4

4/5

```
        ┌─────────────────┐
        │  VERIFY SENSOR  │
        └─────────────────┘
                 │
                 ▼
73 ─┐  ┌─────────────────┐        ┌─────────────────┐ ┌─ 80      ┌─────────────────┐ ┌─ 90
    └──│ GENERATE RANDOM │        │  RECEIVE FROM   │           │  RECEIVE FROM   │
       │     NUMBER      │        │    COMPUTER     │           │     SENSOR      │
       └─────────────────┘        └─────────────────┘           └─────────────────┘
                 │                          │                            │
                 ▼                          ▼                            ▼
74 ─┐  ┌─────────────────┐        ┌─────────────────┐ ┌─ 82      ┌─────────────────┐ ┌─ 92
    └──│  ENCRYPT WITH   │        │  DECRYPT WITH   │           │  DECRYPT WITH   │
       │  COMPUTER PRₖ &  │        │ MANUFACTURER PRₖ │           │ COMPUTER PRₖ &   │
       │ MANUFACTURER PUₖ │        │ & COMPUTER PUₖ   │           │ MANUFACTURER PUₖ │
       └─────────────────┘        └─────────────────┘           └─────────────────┘
                 │                          │                            │
                 ▼                          ▼                            ▼
76 ─┐  ┌─────────────────┐        ┌─────────────────┐ ┌─ 84      ┌─────────────────┐ ┌─ 94
    └──│ SEND TO TRUSTED │        │  MODIFY RANDOM  │           │     VERIFY      │
       │     SENSOR      │        │     NUMBER      │           │  MODIFICATION   │
       └─────────────────┘        └─────────────────┘           └─────────────────┘
                                            │                            │
                                            ▼                            ▼
                            ┌─────────────────┐ ┌─ 86      ┌─────────────────┐
                            │  ENCRYPT WITH   │           │    VERIFIED     │
                            │ MANUFACTURER PRₖ │           └─────────────────┘
                            │ & COMPUTER PUₖ   │
                            └─────────────────┘
                                     │
                                     ▼
                            ┌─────────────────┐ ┌─ 88
                            │ SEND TO COMPUTER │
                            └─────────────────┘
```

FIG. 5

5/5

```
        ┌──────────────┐
        │  AUTHORIZE   │
        └──────────────┘
               │
               ▼
100 ──   ┌──────────────┐        ┌──────────────┐   ── 108
         │    SENSOR    │        │   COMPUTER   │
         │   POWER ON   │        │    SENDS     │
         │  SELF TEST   │        │   INTENDED   │
         │              │        │  RECIPIENT   │
         └──────────────┘        │ PUₖ TO SENSOR│
               │                 └──────────────┘
               ▼                        │
102 ──   ┌──────────────┐               ▼
         │    SENSOR    │        ┌──────────────┐   ── 110
         │ VERIFICATION │        │SENSOR ENCRYPTS│
         │      BY      │        │MESSAGE WITH PRₖ│
         │   COMPUTER   │        │AND RECIPIENT PUₖ│
         └──────────────┘        └──────────────┘
               │                        │
               ▼                        ▼
104 ──   ┌──────────────┐        ┌──────────────┐   ── 112
         │SENSOR MATCHES│        │ SENSOR SENDS │
         │  TEMPLATES   │        │   MESSAGE TO │
         │              │        │   COMPUTER   │
         └──────────────┘        └──────────────┘
               │                        │
               ▼                        ▼
106 ──   ┌──────────────┐        ┌──────────────┐   ── 114
         │SENSOR SELECTS│        │   COMPUTER   │
         │ PRₖ OF ENROLLED│      │  TRANSMITS   │
         │   TEMPLATE   │        │  MESSAGE TO  │
         └──────────────┘        │   INTENDED   │
                                 │  RECIPIENT   │
                                 └──────────────┘
                                        │
                                        ▼
                                 ┌──────────────┐   ── 116
                                 │   INTENDED   │
                                 │RECIPIENT VERIFIES│
                                 │ USING PRₖ AND │
                                 │MANUFACTURER PUₖ│
                                 └──────────────┘
                                        │
                                        ▼
                                 ┌──────────────┐
                                 │  AUTHORIZED  │
                                 └──────────────┘
```

FIG. 6

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04L9/30   H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04L   G06F   G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 832 091 A (SCHMIDT GREGORY J ET AL) 3 November 1998 (1998-11-03) abstract column 2, line 7 - line 37 claims 1-3 figure 2	1-4,6,7, 10-12
P,Y	EP 0 923 018 A (NIPPON ELECTRIC CO) 16 June 1999 (1999-06-16) abstract column 1, line 45 -column 2, line 10 column 3, line 26 - line 44 claim 1 figures 1,3	1-4,6,7, 10-12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 August 2000	16/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

5

Form PCT/ISA/210 (second sheet) (July 1992)

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5832091	A	03-11-1998	US	5541994 A	30-07-1996
			AU	689946 B	09-04-1998
			AU	3339095 A	27-03-1996
			BR	9509002 A	02-06-1998
			CA	2199034 A	14-03-1996
			WO	9608093 A	14-03-1996
			CN	1157677 A	20-08-1997
			EP	0780040 A	25-06-1997
			JP	10505474 T	26-05-1998
			US	5680460 A	21-10-1997
			US	5737420 A	07-04-1998
EP 0923018	A	16-06-1999	JP	11175478 A	02-07-1999
			CN	1220433 A	23-06-1999